WHAT IS CLAIMED IS:

1. A method of authenticating a user ID by making use of a net entry apparatus (40) possessing a cryptography security mechanism to establish two-way communication with an authentication server (20) and an application server (30) through a host computer (10), involving a two stage authentication process, wherein

the first-stage authentication is conducted between the net entry apparatus (40) and the authentication server (20), whereby the authentication server (20) obtains the basic data or user ID from the net entry apparatus (40) to generate a random number test key, and then sends it to the net entry apparatus (40); then the net entry apparatus (40) encrypts the test key with an embedded private key and sends it back to the authentication server (20); then the authentication server (20) retrieves its own copy of the test key, adds an encryption with a symmetrical test key, and compares it with the test key received; then if these two test keys correspond with each other, the authentication server (20) generates a network key and sends it to the host computer (10);

the second-stage authentication is conducted after the network key is received by the authentication server (20), whereby the authentication server (20) generates an encrypted token with the network key and sends it to the host computer (10); then the host computer (10) issues the encrypted token to the application server (30) to which the user intends to gain access; then the application server (30) receiving the encrypted token passes it back to the authentication server (20) for verification; then the authentication server (20) decrypts the returned token with the network key and compares it with the original

token; then if the two tokens correspond with each other, the authentication server (20) notifies the application server (30) that the user ID is valid; otherwise, the user ID is invalid if these two tokens do not match.

2. The method of authenticating a user ID as claimed in claim 1, wherein the first stage authentication further includes:

activating the authentication process;

reading off the basic data or user ID of the net entry apparatus (40), by the host computer (10), and sending it to the authentication server (20);

generating a random number test key, by the authentication server (20), on receiving the user ID of the net entry apparatus (40) and keeping a copy of the random number test key;

encrypting the random number test key using the private key of the net entry apparatus (40), and sending it to the authentication server (20);

retrieving own copy of random number test key, by the authentication server (20) for encryption with the symmetrical copy of the private key, and comparing it with the received test key;

generating a network key, by the authentication server (20), if the two test keys correspond with each other (20).

3. The method of authenticating a user ID as claimed in claim 2, wherein the second stage authentication further includes:

using the network key generated in the first stage authentication to encrypt a token, by the authentication server (20), and passing the encrypted token to the host computer (10);

sending the encrypted token to the application server (30) from the host computer (10);

passing the encrypted token to the authentication server (20) for verification when the application server (30) receives the encrypted token;

decrypting the token with the network key, by the authentication server (20), and comparing it with the original copy of token;

notifying the application server (30) that the user ID is valid for the intended on-line transactions, if these two tokens correspond with each other; or the user is invalid if these two tokens do not correspond.

4. The method of authenticating a user ID as claimed in claim 1, wherein the private key embedded in the net entry apparatus (40) and maintained by the authentication server (20) is created with a high compression security standard of AES 128-256 bits.

5. The method of authenticating a user ID as claimed in claim 2, wherein the private key embedded in the net entry apparatus (40) and maintained by the authentication server (20) is created with a high compression security standard of AES 128-256 bits.

6. The method of authenticating a user ID as claimed in claim 3, wherein the private key embedded in the net entry apparatus (40) and maintained by the authentication server (20) is created with a high compression security standard of AES 128-256 bits.

7. The method of authenticating a user ID as claimed in claim 1, wherein the private key embedded in the net entry apparatus (40) and maintained by the

authentication server (20) is created with regular security standards complying with RSA, DES, 3DES, MD5, MD2, and SHA-1.

8. The method of authenticating a user ID as claimed in claim 2, wherein the private key embedded in the net entry apparatus (40) and maintained by the authentication server (20) is created with regular security standards complying with RSA, DES, 3DES, MD5, MD2, and SHA-1.

9. The method of authenticating a user access to network stations as claimed in claim 3, wherein the private key embedded in the net entry apparatus (40) and maintained by the authentication server (20) is created with regular security standards complying with RSA, DES, 3DES, MD5, MD2, and SHA-1.

10. A net entry apparatus (40) for use in authentication, comprising:

a microprocessor (41) for internal computation;

a connection interface (42) for linking up with the host computer (10);

an encryption unit (43) for creating encrypted data;

a system memory (44) for temporarily saving of user ID of the net entry apparatus (40) and random number test key.

11. The net entry apparatus as claimed in claim 10, wherein the microprocessor (41) is built in with RISC capability.

12. The net entry apparatus as claimed in claim 10, wherein the connection interface (42) has a USB 1.1 or a higher specification.

13. The net entry apparatus as claimed in claim 10, wherein the encryption unit (43) is created with high compression security standards of AES 128-256 bits.

14. The net entry apparatus as claimed in claim 10, wherein the encryption

unit (43) is created with regular security standards complying with RSA, DES, 3DES, MD5, MD2, and SHA-1.

15. The net entry apparatus as claimed in claim 10, wherein the system memory (44) is built with a read only memory, dynamic random access memory, and erasable programmable read-only memory devices.